Security Update 34 Release Notes

symantec™

Security Update 34 Release Notes

Documentation version 34

Legal Notice

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014

http://www.symantec.com

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's maintenance offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers automatic software upgrade protection
- Global support that is available 24 hours a day, 7 days a week
- Advanced features, including Account Management Services

For information about Symantec's Maintenance Programs, you can visit our Web site at the following URL:

www.symantec.com/techsupp/

Contacting Technical Support

Customers with a current maintenance agreement may access Technical Support information at the following URL:

www.symantec.com/techsupp/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system

- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/techsupp/

Customer service

Customer service information is available at the following URL:

www.symantec.com/techsupp/

Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and maintenance contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Maintenance agreement resources

If you want to contact Symantec regarding an existing maintenance agreement, please contact the maintenance agreement administration team for your region as follows:

Asia-Pacific and Japan	contractsadmin@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Additional enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively.

Enterprise services that are available include the following:

Symantec Early Warning Solutions	These solutions provide early warning of cyber attacks, comprehensive threat analysis, and countermeasures to prevent attacks before they occur.
Managed Security Services	These services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.
Consulting Services	Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring, and management capabilities. Each is focused on establishing and maintaining the integrity and availability of your IT resources.
Educational Services	Educational Services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about Enterprise services, please visit our Web site at the following URL:

www.symantec.com

Select your country or language from the site index.

Introducing Security Update 34

This document includes the following topics:

About the Security Updates

The Symantec Enterprise Security Manager (ESM) Security Update Release Notes describe the security updates for Symantec ESM 6.0, 6.1.1, and 6.5.x versions that have been released till date.

What is new in Security Update 34

The following are new in Security Update (SU) 34:

- Support for Windows Server 2008
- Support for Red Hat Enterprise Linux 5.x on IBM z-series (s390x)
- Support for HP-UX 11.23 on HP-UX PA-RISC
- New Agent Information module
- One new check in the Active Directory module on Windows
- Three new checks in the Startup Files module on Windows
- Two new checks in the Account Information module on Windows
- Two new templates in the Startup Files and Active Directory modules
- New columns added in the GPO User Rights, System Services, and Security Options template
- Support for the relational operators in the GPO Security Options and Security Options templates

About the new operating system support

SU 34 provides support for the following operating systems:

- Windows Server 2008
  For more information on how to install/uninstall this agent, see the following URL:
  http://www.symantec.com/avcenter/security/Content/2008.04.04.html
- Red Hat Enterprise Linux 5.x on IBM z-series (s390x)
  For more information on how to install/uninstall this agent, see the following URL:
  http://www.symantec.com/avcenter/security/Content/2007.02.29.html
- HP-UX 11.23 on PA-RISC
  The existing HP-UX 6.5.3 agent has been certified for HP-UX 11.23 on PA-RISC. To use this agent, install the existing HP-UX 6.5.3 agent and apply SU 34 to it.
  Download the HP-UX 6.5.3 agent from the following URL:
  http://www.symantec.com/avcenter/security/Content/2008.02.08.html

About the Agent Information module

A new Agent Information module has been introduced in SU 34. This modules reports information about the following:

- Agent's computer
- SU applied on the agent
- Application Modules installed on the agent

The Agent Information module is supported on all Windows and UNIX operating systems. This module contains eight checks.

Agent name

This check reports the host name of the ESM agent.

This check reports the following message:

Table 1-1 Message for the Agent name check

Message name	Message title	Message severity
ESM_INSTALLED_AGENT	ESM Agent's Name	green-0

Registered to Manager

This check reports all ESM managers to which the agent is registered. All these managers are listed in the /esm/config/manager.dat file.

This check reports the following message:

Table 1-2 Message for the Registered to Manager check

Message name	Message title	Message severity
ESM_REGISTERED_MANAGER	Registered to Manager	green-0

OS information

This check reports the Operating System (OS) name, the OS version, the service pack, and build number of the ESM agent.

This check reports the following messages:

Table 1-3 Messages for the OS information check

Message name	Message title	Message severity
ESM_OS_INFORMATION	OS Information	green-0
ESM_REGISTRY_MISSING	Missing Registry Entry	yellow-2

Note: The message ESM_REGISTRY_MISSING is reported on Windows operating systems only.

Agent version

This check reports the version of the ESM agent.

This check reports the following message:

Table 1-4 Message for the Agent version check

Message name	Message title	Message severity
ESM_AGENT_VERSION	Agent Version	green-0

SU version

This check reports the SU version of the ESM agent.

This check reports the following message:

Table 1-5 Message for the SU version check

Message name	Message title	Message severity
ESM_SU_VERSION	SU Version	green-0

CPU information

This check reports the type of processor, the number of processors, and the frequency of the processor on the agent computer.

This check reports the following messages:

Table 1-6 Messages for the CPU information check

Message name	Message title	Message severity
ESM_CPU_INFO	CPU Information	green-0

Table 1-6 Messages for the CPU information check *(continued)*

Message name	Message title	Message severity
ESM_CPU_PARAM	CPU Parameters	green-0
ESM_REGISTRY_MISSING	Missing Registry Entry	yellow-2

Note: The messages ESM_REGISTRY_MISSING and ESM_CPU_PARAM are reported on Windows operating systems only.

DNS Setting

This check reports the domain name and DNS servers of the ESM agent.

This check reports the following messages:

Table 1-7 Messages for the DNS Setting check

Message name	Message title	Message severity
ESM_PRIMARY_DNSSUFFIX	Primary DNS Suffix	green-0
ESM_DNS_SERVERS	DNS Servers	green-0
ESM_REGISTRY_MISSING	Missing Registry Entry	yellow-2

Note: The messages ESM_PRIMARY_DNSSUFFIX and ESM_REGISTRY_MISSING are reported on Windows operating systems only.

ESM Application Modules

This check reports all the ESM application modules that are installed on the agent.

This check reports the following message:

Table 1-8 Message for the ESM Application Modules check

Message name	Message title	Message severity
ESM_APPLICATION_MODULE	ESM Application Module	green-0

New checks

New checks have been added in the following modules:

- Active Directory
- Startup Files
- Account Information

Active Directory

The following check has been added in the Active Directory module:

- DCOM Machine Restriction
  The DCOM Machine Restriction check reports if the DCOM local policies are enabled or not. It also reports the difference in security descriptor in comparison with the template. This check is supported on Windows Server 2003 (SP1/SP2), Windows XP (SP2), Windows Vista, and Windows Server 2008 operating systems.
  This check reports on the following DCOM local policies:
  - DCOM: Machine Access Restrictions in Security Descriptor Definition Language
  - DCOM: Machine Launch Restrictions in Security Descriptor Definition Language

This check reports the following messages:

Table 1-9 Messages for the DCOM Machine Restriction check

Message Name	Message Title	Message Severity
ESM_DCOM_INCORRECT_VALUE	Incorrect Policy Value	user-defined in template
ESM_INVALID_TEMPLATE_ENTRY	Incorrect Template Entry	red-4
ESM_POLICY_NOT_SET	DCOM Policy not defined	user-defined in template
ESM_SECDESC_NOT_SET	Security Descriptor not set for DCOM Policy	user-defined in template

See "DCOM Machine Restriction template" on page 16.

Startup Files

The following checks have been added in the Startup Files module:

- Data Execution Prevention (Hardware)
- Data Execution Prevention (Software)

- Services Security Options

Data Execution Prevention (Hardware)

Data Execution Prevention (DEP) is a set of hardware technologies that perform additional checks on memory to help prevent malicious code from running on a system.

The Data Execution Prevention (Hardware) check reports on the setting of Data Execution Prevention (DEP).

This check reports a security violation if the following conditions are true:

- DEP is not set to prevent overrun attacks by stopping the execution of the code
- DEP is not set on the drivers

This check is supported on Windows Server 2003 operating systems.

This check reports the following messages:

Table 1-10 Messages for the Data Execution Prevention (Hardware) check

Message Name	Message Title	Message Severity
ESM_DEPAVAILABLE	DEP Available	red-4
ESM_DEPDRIVERS	DEP Drivers	red-4

Data Execution Prevention (Software)

Data Execution Prevention (DEP) is a set of software technologies that perform additional checks on memory to help prevent malicious code from running on a system.

The Data Execution Prevention (Software) check reports on the setting of Data Execution Prevention (DEP).

This check reports a security violation if one of the following DEP settings is currently applied:

- Always On
- Always Off

This check reports relevant information if one of the following DEP settings is currently applied:

- Opt In
- Opt Out

This check is supported on Windows Server 2003 operating systems.

This check reports the following message:

Table 1-11 Message for the Data Execution Prevention (Software) check

Message Name	Message Title	Message Severity
ESM_DEPSUPPOLICY	DEP Support Policy	yellow-1
ESM_DEPSUPPOLICY_G	DEP Support Policy	green-0

Services Security Options

The Services Security Options check reports on the local service startup and service permissions. This check is supported on all Windows operating systems.

This check reports the following messages:

Table 1-12 Messages for the Services Security Options check

Message Name	Message Title	Message Severity
ESM_INVALID_TEMPLATE_ENTRY	Incorrect Template Entry	red-4
ESM_SERVICE_ACL_ERROR	Error reporting system services ACL	red-4
ESM_TEMPLATE_NOT_FOUND	Template file not found	red-4
ESM_INCORRECT_VALUE	Security Services Options Incorrect Value	user-defined in template
ESM_SERVICE_STARTUP_ERROR	Error reporting system services startup	red-4
ESM_INVALID_SERVICE	Service does not exist	red-4
ESM_FILE_MISSING	No template files specified	red-4

See "System Services template" on page 17.

Account Information

The following checks have been added in the Account Information module:

- Enumerate groups on Domain Controller

- Enumerate groups on member server

Enumerate groups on Domain Controller

The Security groups and their users check reports the nested security groups and the users in each group on Domain Controller and trusted domain when the Enumerate groups on Domain Controller check is enabled. This check is supported on Windows 2000/Server 2003/Server 2008 operating systems.

If you do not enable the Enumerate groups on Domain Controller check, the Security groups and their users check reports the members that are assigned explicitly to each group.

This check reports the following message:

Table 1-13 Message for the Enumerate groups on Domain Controller check

Message Name	Message Title	Message Severity
ESM_GROUP_AND_USER	Security group member	green-0

Enumerate groups on member server

The Security groups and their users check reports nested security groups and all users in each group on member server when the Enumerate groups on member server check is enabled.

If you do not enable the Enumerate groups on member server check, the Security groups and their users check reports the members that are assigned explicitly to each group.

On servers, this check is supported on Windows 2000/Server 2003/Server 2008 operating systems. On the workstations, this check is supported on Windows XP/Vista operating systems.

This check reports the following message:

Table 1-14 Message for the Enumerate groups on member server check

Message Name	Message Title	Message Severity
ESM_GROUP_AND_USER	Security group member	green-0

New templates

The following new templates have been added in SU 34:

- DCOM Machine Restriction
- System Services

DCOM Machine Restriction template

The DCOM Machine Restriction template has been added for the DCOM Machine Restriction check that is available in the Active Directory module.

This template contains the following fields:

Check Enabled	Select this option to report on the permissions for the policy specified in the Policy field
Severity	Specify the severity of the messages reported for this object The available options are Red, Green, and Blue.
Policy	Select the policy that you need to report on You can select one of the following policies: ■ DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) Syntax ■ DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) Syntax

Permissions ACL	Use this sublist to specify the users/groups and the permissions that are allowed/denied to them You can specify the following permissions for the DCOM: Machine Access Restrictions policy: ■ DC: Local Access ■ LC: Remote Access You can specify the following permissions for the DCOM: Machine Launch Restrictions policy: ■ DC: Local Launch ■ LC: Remote Launch ■ SW: Local Activation ■ RP: Remote Activation **Note:** You need to specify the abbreviated format of these permissions. The following are examples of how you specify the permissions: ■ If the Everyone user has Local Access and Remote Access permissions, the entry looks as follows: Everyone : CCDCLC : Allow ■ If the Everyone user has Local Launch, Remote Launch, Local activation, and Remote activation permissions, the entry looks as follows: Everyone : CCDCLCSWRP : Allow

System Services template

The System Services template has been added for the Services Security Options check that is available in the Startup Files module.

This template contains the following fields:

Check Enabled	Select this option to report on the system service specified in the Service Name field

Service Name	Specify the actual service name or the executable name that is present in the properties of the service in the Control Panel To find a service name, do the following: ■ On the Windows taskbar, click Start. ■ Click Settings > Control Panel > Administrative Tools > Services. ■ Right-click the service that you need in the Name column. ■ Click Properties. The correct service name is in the Service Name field of the Properties window.
Service Display Name	Specify the service name that is displayed This name can simply be a description of the service. **Note:** When you create your template, you must include both the Service Name and the Service Display Name in the template or you will receive an error message.
Startup	Specify if the service starts automatically, manually, or is disabled The available options are Automatic, Manual, and Disabled.
Severity	Specify the severity of the messages reported for this object The available options are Red, Green, and Blue.
Permissions ACL Check Enabled	Select this option if you want to report on the permissions specified in the Permissions ACL field

Permissions ACL	Use this sublist to specify the users/groups and the permissions that are allowed/denied to them You can specify the following permissions: ■ C : Read Permissions ■ P : Change Permissions ■ O : Take Ownership ■ H : Change template ■ E : Enumerate Dependents ■ I : Interrogate ■ A : Pause and Continue ■ Q : Query template ■ R : Query Status ■ S : Start ■ T : Stop ■ U : User-Defined Control ■ D : Delete **Note:** You need to specify the abbreviated format of these permissions. The following are examples of how you specify the permissions: ■ For an Administrator with Full Control, the entry looks as follows: %Administrators% : QHRESTAIUDCPO : Allow ■ For a user with Read permissions, the entry looks as follows: %INTERACTIVE% : QREIUC : Allow

Modified checks

The following checks have been modified:

- System Services (Group Policy)
- Accounts can be locked (Account Integrity)
- Login retries (Login Parameters)
- Shutdown without logon (Login Parameters)
- Users without system password strength (Password Strength)
- Password length restrictions (Password Strength)
- Minimum password history (Password Strength)

- Password age warning (Password Strength)
- Check critical processes (Startup Files)

System Services

The System Services check in the Group Policy module has been modified to report on the permissions of system services.

The following messages have been added to this check:

Table 1-15 Messages for the System Services check

Message Name	Message Title	Message Severity
ESM_INVALID_TEMPLATE_ENTRY	Incorrect Template Entry	red-4
ESM_SERVICE_ACL_ERROR	Error reporting system services ACL	red-4

Accounts can be locked

The Accounts can be locked check in the Account Integrity module has been modified to report for the Linux and Solaris operating systems.

Login retries

The Login retries check in the Login Parameters module has been modified to report for the Linux and Solaris operating systems.

Shutdown without logon

The following message has been added to the Shutdown without logon check in the Login Parameters module:

Table 1-16 Message for the Shutdown without logon check

Message Name	Message Title	Message Severity
ESM_NO_SHUTDOWN_FROM_LOGON	Shutdown from Logon not defined	yellow-1

This message is reported if the registry key for the Shutdown without logon option is not defined in the registry.

Users without system password strength

The following message has been added to the Users without system password strength check for non-trusted HP-UX operating systems:

Table 1-17 Message for the Users without system password strength check

Message Name	Message Title	Message Severity
STKU_NOTSUPPORT_STRENGTH	User without system password strength not supported	green-0

Password length restrictions

The Password length restrictions check in the Password Strength module has been modified to report on the SuSE Linux operating systems.

Minimum password history

The following message has been added to the Minimum password history check in the Password Strength module for non-trusted HP-UX versions 11 and later operating systems:

Table 1-18 Message for the Minimum password history check

Message Name	Message Title	Message Severity
STKU_NOTSUPPORT_HISTSIZE	Minimum Password History not supported	green-0

Password age warning

The Password age warning check in the Password Strength module has been modified to report on the HP-UX operating systems in the shadow mode.

Check critical processes

The Check critical processes check in the Startup files module has been modified to apply only on non-global zones that are created on Sun Solaris 10+ with esm agent installed on non-global zones and if any/all of the following checks are enabled:

- Duplicate processes

- Installed services
- Services not in template

Modified templates

New columns have been added to the following templates:

- GPO User Rights
- GPO System Services
- Security Options

GPO User Rights

A new column named Required has been added to the Users/Groups sublist in the GPO User Rights Template.

This column has the following options:

Mandatory	Specifies that the user/group must exist
Prohibited	Specifies that the user/group must not exist
Optional	Specifies that the user/group may/may not exist

GPO System Services

The following new columns have been added to the GPO System Services template:

Permissions ACL check enabled	If checked, enables the Permissions ACL check to run on the system services
Permissions ACL	Specifies the users/groups along with the permissions that they should have on the system services You need to specify abbreviated forms of the permissions in the sublist. See "System Services template" on page 17.

Security Options

A new column named Skip Conditions has been added to the Security Options template for Windows operating systems. The column is of the type sublist.

In the sublist for Skip Conditions, you can specify conditions for registry keys/values/data. Based on these conditions, the messages for that object are not reported by ESM.

Resolved issues

The following issues are resolved in SU 34:

Agent Information	A new Agent Information module has been introduced in SU 34. This module provides agent information such as the agent's version, the manager it is registered to, the SU version running on the agent, and so on. See "About the Agent Information module" on page 9.
OS Patches (AIX)	The Installed patches check has been modified to report correctly when the fileset information is provided in the OS patches template.
Login Parameters (Windows)	The Shutdown without logon check used to report the shutdownwithoutlogon key as disabled if it was not defined at HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system. The check now reports the following message if the key is not defined: The registry value is not defined for Shutdown from Logon option.
Login Parameters (HP-UX)	The Login Parameters module has been enhanced to support HP-UX operating systems in shadow mode version 11iv1onwards.
Login Parameters (SuSE Linux 10)	The Login Parameters module now correctly reports the logging configuration information from the syslog-ng configuration file.
Login Parameters (Linux)	The signal 6 error no longer appears if the data in the /var/log/messages file is not in the expected format after you run the Login Parameters module.
Registry (Windows)	The Registry template now correctly processes the registry values that contain tab spaces.
File Find (Solaris 10)	The Global zone only check has been modified and it no longer reports files from the non-global zones.

Startup Files (Solaris 10)	The Critical processes and Installed services checks have been modified to report the mandatory processes that are specified in the template for Solaris 10 zones only.
Startup Files /OS Patches/File Find/File Attributes/Password Strength/File Watch(Windows)	Previously, ESM_startup.log file used to get created in the C drive for some modules. This file used to take up a considerable amount of space on the hard disk. These modules have been modified and this log file no longer gets created.
Startup Files (HP-UX)	The Startup Files module has been enhanced to support HP-UX operating systems in shadow mode version 11iv1onwards for Enhanced security mode check.
Active Directory (Windows)	A new column named Skip Conditions has been added to the Security Options template for Windows operating systems. The column is of the type sublist. In the sublist for Skip Conditions, you can specify conditions for registry keys/values/data. Based on these conditions, the messages for that object are not reported by ESM.
OS Patches (Windows)	The OS Patches module has been modified and it no longer reports the "Cannot determine patch status" message if the Relaxed or Strict option is enabled. The module now displays the expected result.
Account Integrity (Linux)	The Disabled accounts check now also reports the accounts whose passwords are not set.
Account Integrity (All UNIX)	The Account should be disabled check now also reports the user accounts that are set to No Login (NL).
Account Integrity (HP-UX)	The Account Integrity module has been enhanced to support HP-UX operating systems in shadow mode version 11iv1onwards for Password in /etc/passwd check.
Account Integrity (Red Hat Enterprise Linux Opteron and SuSE 10 Itanium)	The Reserved UID/GID check has been modified and it no longer reports a signal 11 error when run on Red Hat Enterprise Linux (Opteron) and SuSE 10 (Itanium) operating systems.

File Attributes (Solaris)	The invalid entries such as /etc/.../var/adm/wtmpx in the sysstart.sol template has been removed for the File Attributes module to work correctly.
System Auditing (Solaris)	The System Auditing module has been modified to detect the audit entries for Solaris operating systems in the Event Maps and Events templates.
Password Strength (Windows)	The Password Strength no longer generates unnecessary security events in the Event Viewer while enumerating the Domain Controller or the Member Server user accounts.

The following issues have been resolved for the Password Strength module on UNIX operating systems:

- The Password Strength module has been enhanced to support HP-UX operating systems in shadow mode version 11iv1onwards.
- The performance of the Password Strength module has been improved by 30-35 % on Solaris operating systems.
- The Password Strength module has been modified to identify the LDAP setting on the PAM module on the authentication server on Solaris operating systems.
- The Information field on the console now displays correct messages when the checks that are specific to trusted HP-UX systems are run on non-trusted HP-UX systems.

  Note: The suppressions, if any, that you applied on the old message will no longer be available since the message has now changed.

- The Password Strength module no longer reports the Invalid minimum password history message on the non-trusted HP-UX operating systems if they do not support minimum password history.
- The Maximum password age, Minimum password age, and Minimum length restrictions checks now report correctly if there is space between the attribute and the value in the /etc/login.defs file on the SUSE Linux 10 (x86) agents.
- The Password requirements template no longer processes the commented lines in the files that are uploaded by using the Add File option.
- The Password Strength module now displays the correct configuration file name for the Password length restrictions check in the Names column of the message that is displayed on the console for Solaris and HP-UX operating systems.

Note: The suppressions, if any, that you applied on the old message will no longer be available since the message has now changed.

- The Password Strength module no longer reports an unexpected system error if the following parameters are removed from the password configuration file on AIX operating systems:
  - histsize
  - maxage
  - minage
  - dictionlist

  The following new messages are now reported for these parameters:
  - hitsize - Invalid minimum password history
  - maxage - Invalid maximum password age
  - minage - Invalid minimum password age
  - dictionlist - Users without system password strength
- The Password length restrictions check no longer reports the Invalid minimum password length message on the HP-UX operating systems if they do not support the check.
- The Minimum password length now reports correctly on SuSE Linux (64-bit, Itanium) operating systems.
- The Password Strength module no longer reports an unexpected system error for the users whose entries have been removed from the shadow file on Solaris and HP-UX operating systems.
- The Maximum password age check no longer reports on the accounts that are locked.
- The Guessed passwords check, when selected in combination with the Repeating characters check, now reports the password in the following format in the Information field on the console:
  <first_character>*<last character>
- The Maximum password age check now reports the following message if the MAXWEEKS parameter in the /etc/default/passwd file is set to 0 on Solaris operating systems:
  The system default password maximum age is not set or is set to 0.

- The Minimum password age check now reports the following message if the MINWEEKS parameter in the /etc/default/passwd file is set to 0 on Solaris operating systems:
  The system default password minimum age is not set or is set to 0.
- On HP-UX operating systems, the Minimum password age check now correctly reports the accounts who have set their minimum password age to less that the age specified in the name list.
- The System generated password check now correctly reports on those accounts whose passwords are system-generated.

Known issues

The following issues are known in SU 34:

Agent Information	The Registered to manager check might report the managers that have been uninstalled or the managers with which the agent is not registered anymore. To resolve this issue, delete the entries of such managers manually, and rerun the check.
Agent Information (AIX RS6k)	The CPU information check is unable to identify the processor type and the number of processors on AIX RS6k operating systems.
Response (All Windows and UNIX)	The Response module is no longer supported SU 34 onwards.
OS Patches (HP-UX)	The OS Patches module reports an unhandled exception on the console if the parameter maxdsiz is set to the default value of 64 MB. To resolve this issue, set the value of maxdsiz to 256 MB by using the SAM's utility.
LiveUpdate (SuSE Linux 10 Itanium/Red Hat Enterprise Linux Itanium)	LiveUpdate to the SU on SuSE 10 (Itanium) might fail if libreadline.so.4 and libtermcap.so.2 are not present. LiveUpdate to the SU on Red Hat Enterprise Linux (Itanium) might fail if libreadline.so.4 is not present. To resolve this issue, apply the tpk to upgrade to SU.
LiveUpdate	ESM might generate an error when you transfer the LiveUpdate packages for SU 34 from the console to the manager. Ignore this error as the packages get transferred successfully.

System requirements

Symantec reserves the right to certify the Security Update on the new versions of these operating systems before officially supporting them.

Table 1-19 lists the supported operating systems for SU 34.

Table 1-19 Supported operating systems for SU 34

Agent operating system	Platform	Supported versions on 6.0	Supported versions on 6.5.x
AIX	RS 6000	N/A	5.2 (32-bit and 64-bit) 5.3 (32-bit only)
AIX	PPC 64	5.3 (64-bit only)	5.3 (64-bit only)
ESX Server	x86, Opteron	N/A	3.0.2 (supported on 6.5.3 only)
HP-UX	HPPA	10.20/11.0/11.11	11.0/ 11.11
HP-UX	HPPA	N/A	11.23 (supported on 6.5.3/6.5.3 SP1/6.5.3 SP2 only)
HP-UX	Itanium®	11.23	11.23
Red Hat Enterprise Linux	IBM z-series (s390x)	N/A	5.x (supported on 6.5.3 only)
Red Hat Enterprise Linux ES	x86, Opteron and EM64T	3.0	3.0/4.0
Red Hat Enterprise Linux ES	x86, Opteron, EM64T, and IA64	N/A	5.0/5.1
Red Hat Enterprise Linux WS and AS	x86, Opteron and EM64T	3.0	3.0/4.0
Red Hat Enterprise Linux AS	Itanium®	3.0	3.0/4.0
Sun Solaris	SPARC	2.8/2.9/2.10	2.8/2.9/2.10
Sun Solaris	x86, Opteron and EM64T	N/A	2.10

Table 1-19 Supported operating systems for SU 34 *(continued)*

Agent operating system	Platform	Supported versions on 6.0	Supported versions on 6.5.x
SUSE Linux Standard Server	x86	N/A	9
SUSE Linux Enterprise Server	x86	9	9/10
SUSE Linux Enterprise Server	Itanium®	9	9/10
SUSE Linux Enterprise Server	Opteron and EM64T	N/A	9/10 (supported on 6.5.3/6.5.3 SP1/6.5.3 SP2 only)
SUSE Linux Enterprise Server	IBM PPC e-Server	N/A	9/10
Windows 2000 Professional and Server	x86	All	All
Windows Server 2003	x86	All	All
Windows Server 2003	Itanium®	All	All
Windows Server 2003 Enterprise	Opteron and EM64T	N/A	All
Windows Vista	x86	N/A	All
Windows Vista	Opteron and EM64T	N/A	All
Windows XP Professional	x86	SP2	SP2
Windows Server 2008	x86	N/A	All (supported on 6.5.3 only)
Windows Server 2008	Opteron and EM64T	N/A	All (supported on 6.5.3 only)
Windows Server 2008	Itanium®	N/A	All (supported on 6.5.3 only)

Table 1-19 Supported operating systems for SU 34 *(continued)*

Agent operating system	Platform	Supported versions on 6.0	Supported versions on 6.5.x
Windows Server 2008 Core Installation	x86	N/A	All (supported on 6.5.3 only)
Windows Server 2008 Core Installation	Opteron and EM64T	N/A	All (supported on 6.5.3 only)

Table 1-20 lists the post-install disk space usage for an ESM 6.5 agent with SU34 applied. The amount of disk space required by each agent depends on its operating system.

Table 1-20 Post-install agent disk space requirements for SU 34

Agent operating system	Disk space required (in MB)
AIX /RS 6000	211
AIX 5.3 (PPC)	212
HP-UX (PA-RISC)	126
HP-UX (Itanium®)	128
Red Hat Enterprise Linux ES (x86)	79
Red Hat Enterprise Linux WS and AS (AMD64)	86
Red Hat Enterprise Linux AS (Itanium®)	109
Red Hat Enterprise Linux WS and AS (EM64T)	90
Red Hat Enterprise Linux on IBM z-series (s390x)	98
Sun Solaris 2.8/2.9 (SPARC)	99
Sun Solaris 10 (SPARC)	103
Sun Solaris 10 (x86, Opteron and EM64T)	75
SUSE Linux Enterprise Server 9 (x86)	75
SUSE Linux Enterprise Server 9 (Itanium®)	94
SUSE Linux Enterprise Server on IBM PPC e-Server	74

Table 1-20 Post-install agent disk space requirements for SU 34 *(continued)*

Agent operating system	Disk space required (in MB)
SUSE Linux Enterprise Server (Opteron and EM64T)	137
Windows 2000 Professional and Server (x86)	86
Windows Server 2003 (x86)	86
Windows Server 2003 (Itanium®)	149
Windows Server 2003 Enterprise (Opteron and EM64T)	70
Windows XP Professional (x86)	84
Windows Vista (x86)	43
Windows Vista (Opteron and EM64T)	82
Windows Server 2008 (x86)	56
Windows Server 2008 (Itanium®)	140
Windows Server 2008 (Opteron and EM64T)	79
Windows Server 2008 Core Installation (x86)	56
Windows Server 2008 Core Installation (Opteron and EM64T)	94